



OSINT + ARCO + PROTECCIÓN DE DATOS

# MAPA-RD: Exposición y Ruta de Cierre

---

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

**Felipe Miramontes · Reporte RPT-2026-002 · 2026-01-12**

Reporte Ejecutivo de Seguridad · Exposición pública · Estrictamente Confidencial

# Índice de Riesgo Digital

94

RIESGO MÁXIMO

---

VECTORES DE VULNERABILIDAD

---

ACTIVO:  
Sector Financiero

TIPO:  
Identidad Bancaria

EXPOSICIÓN:  
Filtración Masiva  
(2014/2022)

#### RUTA DE CIERRE

1. Activar alertas biométricas en banca móvil.
2. Revisar historial crediticio (Buró de Crédito) inmediatamente.
3. Solicitar renovación de tarjetas y credenciales bancarias.

#### IMPACTO

- Robo de Identidad Bancaria y Fiscal (RFC).
- Ingeniería Social dirigida de alta precisión.
- Riesgo de extorsión o fraude telefónico.

#### DESCRIPCIÓN DEL EVENTO

Exposición crítica de datos personales y financieros incluyendo saldos de cuenta, RFC, domicilio físico y números de teléfono. Esta información facilita el robo de identidad y fraude bancario directo.

ACTIVO:  
Identidad Digital

TIPO:  
Botnet Logs

EXPOSICIÓN:  
Credential Stuffing (2025)

#### RUTA DE CIERRE

1. Cambio global de contraseñas de manera inmediata.
2. Uso gestor de contraseñas para evitar reutilización.
3. Habilitar 2FA/MFA en todos los servicios críticos.

#### IMPACTO

- Compromiso automatizado de cuentas en diversos servicios.
- Evasión de controles de seguridad básicos.
- Acceso no autorizado persistente.

#### DESCRIPCIÓN DEL EVENTO

El correo y contraseñas asociadas aparecen en listas de amenazas activas de 'Credential Stuffing' (Synthient). Esto indica que los datos están siendo probados activamente contra múltiples servicios.

# 000webhost: Contraseñas en Texto Plano

88 MÁXIMO

ACTIVO:  
Hosting Web

TIPO:  
Servicio de  
Infraestructura

EXPOSICIÓN:  
Texto Plano (2015)

## RUTA DE CIERRE

1. Abandonar el uso de esa contraseña específica definitivamente.
2. Verificar integridad de sitios web antiguos.
3. Monitorear accesos no reconocidos.

## IMPACTO

- Acceso inmediato a cuentas con la misma contraseña.
- Rastreo de actividad por dirección IP.
- Compromiso de sitios web alojados.

## DESCRIPCIÓN DEL EVENTO

Filtración de base de datos completa exponiendo contraseñas almacenadas en texto plano, junto con nombres y direcciones IP. Permite acceso directo sin necesidad de descifrado.

ACTIVO:  
Cuenta Adobe ID

TIPO:  
Software SaaS

EXPOSICIÓN:  
Base de Datos (2013)

#### RUTA DE CIERRE

1. Actualizar cuenta de Adobe si sigue activa.
2. No utilizar pistas de contraseña que revelen información real.

#### IMPACTO

- Deducción de patrones de contraseñas personales.
- Ataques dirigidos a cuentas creativas/profesionales.
- Spam y phishing dirigido.

#### DESCRIPCIÓN DEL EVENTO

Brecha histórica masiva exponiendo usuarios, contraseñas cifradas y, críticamente, las pistas de contraseña (password hints) en texto plano, lo que facilita la deducción de claves.

ACTIVO:

Identidad Digital

TIPO:

Mercado Negro

EXPOSICIÓN:

Agregador de Brechas  
(2016)**RUTA DE CIERRE**

1. Eliminar cuentas en desuso.
2. Verificar actividad en correos secundarios.

**IMPACTO**

- Alta probabilidad de intentos de acceso automatizados.
- Reutilización de credenciales en servicios bancarios/correo.

**DESCRIPCIÓN DEL EVENTO**

Aparición en 'Combo Lists' utilizadas por cibercriminales para ataques de fuerza bruta automatizados contra múltiples plataformas.

ACTIVO:

Múltiples Servicios

TIPO:

Agregador de Brechas

EXPOSICIÓN:

Data Dump Masivo (2019)

**RUTA DE CIERRE**

1. Higiene digital completa: cambio masivo de claves.
2. Uso estricto de gestor de contraseñas.

**IMPACTO**

- Exposición universal a actores de amenaza.
- Saturación de intentos de login.
- Venta de datos en lotes masivos.

**DESCRIPCIÓN DEL EVENTO**

Su correo forma parte de una de las colecciones más grandes de credenciales robadas (773 millones de registros Unique), distribuidas ampliamente en foros de hacking.



ACTIVO:

Productividad

TIPO:

Software SaaS

EXPOSICIÓN:

Base de Datos (2020)

**RUTA DE CIERRE**

1. Revisar documentos almacenados en la nube de Nitro.
2. Cambiar contraseña y desvincular sesiones.

**IMPACTO**

- Espionaje corporativo o personal.
- Acceso a documentos sensibles almacenados.
- Fraude documental.

**DESCRIPCIÓN DEL EVENTO**

Compromiso de servicio de gestión documental. Además de credenciales, existe riesgo sobre metadatos de documentos procesados.

ACTIVO:  
Banco de Imágenes

TIPO:  
Servicio Web

EXPOSICIÓN:  
Base de Datos (2020)

#### RUTA DE CIERRE

1. Verificar privacidad en redes sociales.
2. Estar alerta ante correos/llamadas sospechosas.

#### IMPACTO

- Doxing (publicación de datos privados).
- Acoso o localización física.
- Suplantación de identidad verificada.

#### DESCRIPCIÓN DEL EVENTO

Filtración que incluye direcciones físicas, teléfonos y direcciones IP, combinados con datos de cuenta. Aumenta la superficie para ataques de ingeniería social.

ACTIVO:  
Salud / Lifestyle

TIPO:  
Aplicación Móvil

EXPOSICIÓN:  
Brecha Masiva (2018)

#### RUTA DE CIERRE

1. Cambiar contraseña si es compartida.
2. Desvincular integraciones con redes sociales.

#### IMPACTO

- Perflado de usuario para marketing o estafas.
- Acceso lateral a otras cuentas.

#### DESCRIPCIÓN DEL EVENTO

Exposición de correos, usuarios y contraseñas. Aunque no incluye datos financieros, permite correlacionar hábitos y rutinas del usuario.

ACTIVO:  
Diseño Gráfico

TIPO:  
SaaS

EXPOSICIÓN:  
Base de Datos (2019)

#### RUTA DE CIERRE

1. Cambiar contraseña y activar MFA.
2. Revisar actividad reciente en la cuenta.

#### IMPACTO

- Correlación geográfica.
- Ataques de phishing temáticos (diseño/marketing).

#### DESCRIPCIÓN DEL EVENTO

Exposición de datos de usuario, ubicación geográfica y hashes de contraseña.

ACTIVO:  
Edición de Video

TIPO:  
SaaS

EXPOSICIÓN:  
Base de Datos (2018)

#### RUTA DE CIERRE

1. Monitorear preguntas de seguridad en otros servicios.

#### IMPACTO

- Uso de fecha de nacimiento para recuperar otras cuentas.
- Suplantación de identidad básica.

#### DESCRIPCIÓN DEL EVENTO

Inclusión de fechas de nacimiento y geolocalización junto a credenciales. La fecha de nacimiento es un dato crítico para verificaciones de seguridad.

ACTIVO:

Almacenamiento Cloud

TIPO:

Infraestructura

EXPOSICIÓN:

Base de Datos (2012)

**RUTA DE CIERRE**

1. Asegurar que la contraseña fue cambiada post-2016.
2. Activar 2FA en Dropbox obligatoriamente.

**IMPACTO**

- Intento de descifrado de hashes antiguos.
- Reutilización histórica.

**DESCRIPCIÓN DEL EVENTO**

Brecha antigua pero relevante por la popularidad del servicio. Se filtraron hashes de contraseñas.

ACTIVO:  
Email Personal

TIPO:  
Campaña de Amenaza

EXPOSICIÓN:  
Target List (2023)

#### RUTA DE CIERRE

1. Extrema precaución con adjuntos y enlaces.
2. Mejorar filtros de spam/seguridad en el correo.

#### IMPACTO

- Recepción de correos maliciosos altamente personalizados.
- Riesgo de infección por malware.

#### DESCRIPCIÓN DEL EVENTO

Su dirección de correo ha sido identificada en listas de objetivos de la campaña de phishing 'Manipulated Caiman', enfocada en usuarios de México.

ACTIVO:  
Desarrollo Profesional

TIPO:  
Scraping

EXPOSICIÓN:  
Base de Datos (2016)

#### RUTA DE CIERRE

1. Verificar legitimidad de reclutadores.

#### IMPACTO

- Ofertas de trabajo falsas (Job Scams).
- Ingeniería social basada en perfil laboral.

#### DESCRIPCIÓN DEL EVENTO

Exposición de datos profesionales: habilidades, experiencia y ubicación. Útil para reclutadores falsos o ingeniería social corporativa.



ACTIVO:  
Red Social

TIPO:  
Perfil Público

EXPOSICIÓN:  
Scraping/API (2021)

#### RUTA DE CIERRE

1. Desvincular teléfono/email de la búsqueda pública.
2. Usar alias de correo para redes sociales.

#### IMPACTO

- Desanonimización de cuentas.
- Acoso selectivo.
- Correlación de identidad cruzada.

#### DESCRIPCIÓN DEL EVENTO

Asociación del correo electrónico con el perfil de Twitter (X). Permite vincular la identidad seudónima con la real.

ACTIVO:  
Gestión de Proyectos

TIPO:  
SaaS

EXPOSICIÓN:  
Scraping (2024)

#### RUTA DE CIERRE

1. Hacer tableros privados si contienen datos sensibles.
2. Ignorar correos genéricos de soporte de Trello.

#### IMPACTO

- Phishing temático de Atlassian/Trello.
- Confirmación de cuenta activa.

#### DESCRIPCIÓN DEL EVENTO

Confirmación de que el correo tiene una cuenta de Trello asociada mediante enumeración de API.

# Anexo Técnico

## Índice de Riesgo del Vector (IRV)

El **IRV** es la métrica fundamental de urgencia. No mide el riesgo teórico, sino la necesidad operativa de cierre. Se calcula internamente mediante un modelo ponderado de seis dimensiones.

### FÓRMULA DE CÁLCULO

$$\text{IRV} = [ \Sigma (\text{Componente} \times \text{Peso}) / \Sigma (\text{Peso Máximo}) ] \times 100$$

### Variables del Modelo

#### Criticidad (CA)

x4

Importancia crítica del activo para la continuidad del negocio.

#### Exposición (ET)

x3

Ventana de tiempo y vigencia actual del hallazgo.

#### Superficie (SE)

x3

Facilidad de acceso desde redes públicas o privadas.

#### Impacto (IM)

x4

Suma de impactos (Financiero, Legal, Operativo, Reputacional).

#### Explotación (FE)

x3

Recursos y complejidad técnica requerida para el ataque.

#### Detección (DV)

x3

Probabilidad de evasión de sistemas de monitoreo.

## Índice de Riesgo Digital (IRD)

El **IRD** es el indicador de postura global. Se deriva dinámicamente de los vectores activos mediante un promedio ponderado por severidad.

AGREGACIÓN PONDERADA

$$\text{IRD} = \frac{\sum (\text{IRV} \times \text{Peso Severidad})}{\sum (\text{Pesos Severidad})}$$

Matriz de Pesos

  
**BAJO**  
Multiplicador x1

  
**MEDIO**  
Multiplicador x2

  
**ALTO**  
Multiplicador x3

  
**CRÍTICO**  
Multiplicador x4

  
**MÁXIMO**  
Multiplicador x5